DoD Information Security Policy in an Information Sharing Environment

April 7, 2008

Ms. Anne Schiffiano

Approved for Public Release
U.S. Government Work (17 USC§105) Not copyrighted in the U.S.

INFORMATION SECURITY IN AN INFORMATION SHARING ENVIRONMENT

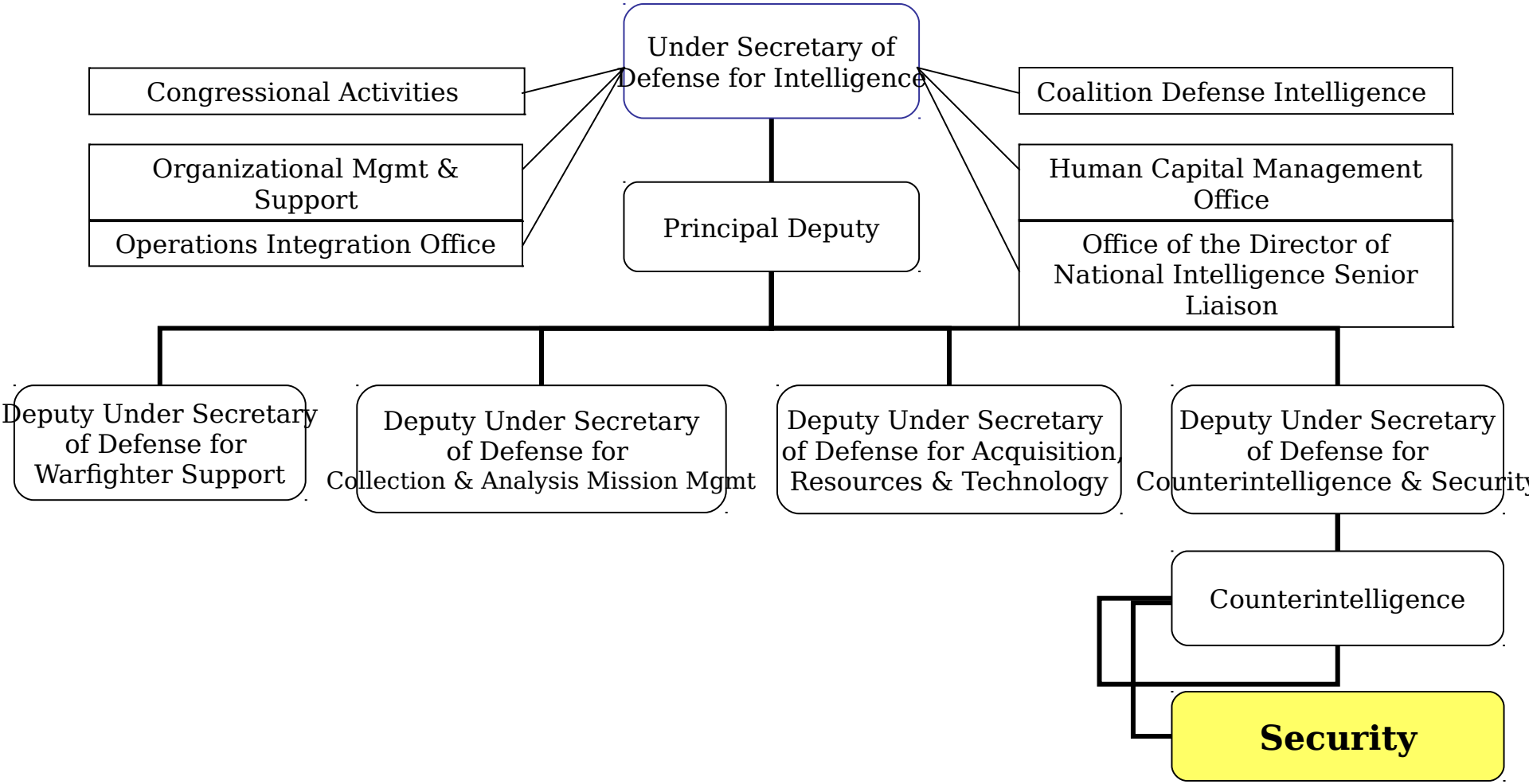
Deborah Ross
Deputy Director, Information Security Policy
Office of the Under Secretary of Defense (Intelligence)

7 April 2008

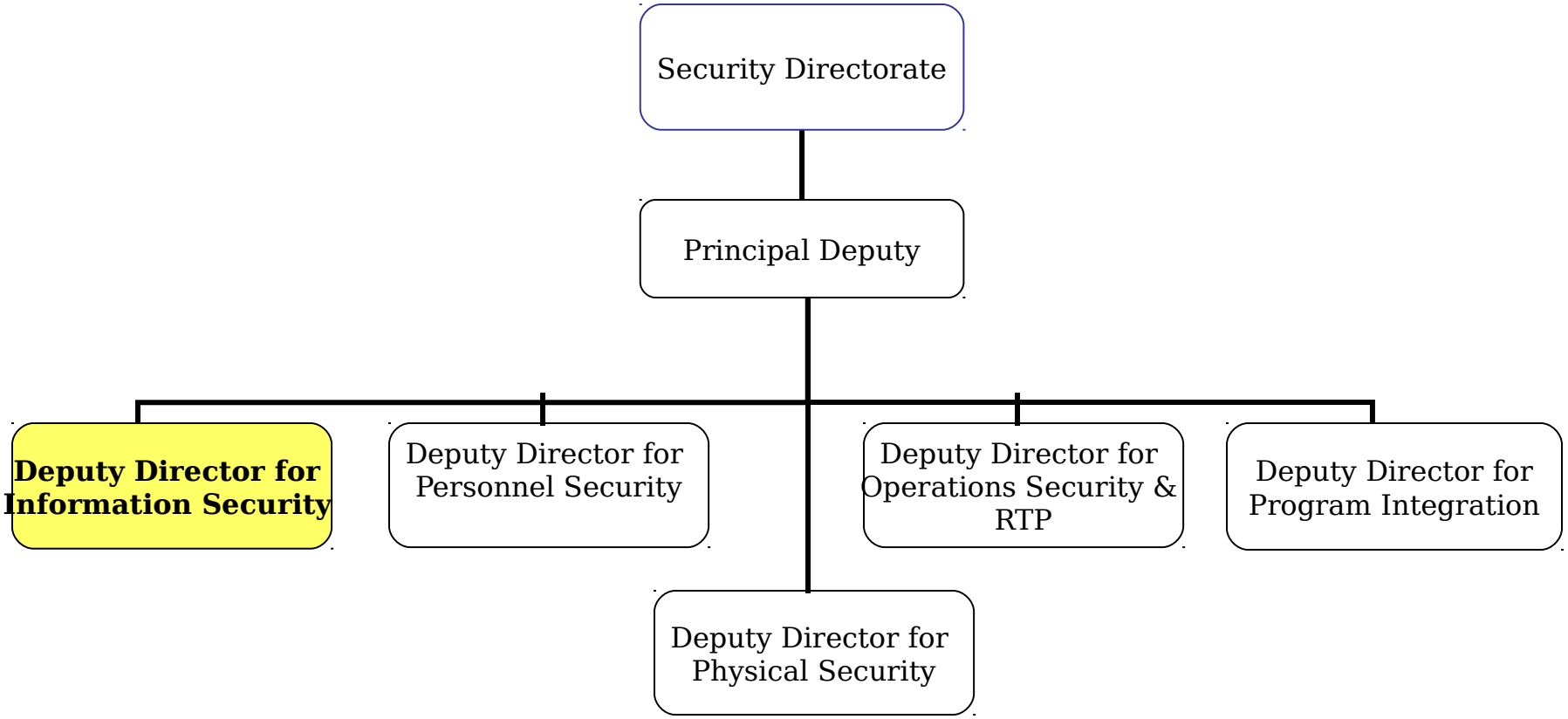
Overview

- Organization
- Responsibilities
- Information Security Role in the Information Sharing Environment (ISE)
- Initiatives
- Your Role

Organization


Under Secretary of Defense for Intelligence
Congressional Activities
Organizational Mgmt & Support
Operations Integration Office
Principal Deputy
Coalition Defense Intelligence
Human Capital Management Office
Office of the Director of National Intelligence Senior Liaison
Deputy Under Secretary of Defense for Warfighter Support
Deputy Under Secretary of Defense for Collection & Analysis Mission Mgmt
Deputy Under Secretary of Defense for Acquisition, Resources & Technology
Deputy Under Secretary of Defense for Counterintelligence & Security
Counterintelligence
Security

Security Directorate


Security Directorate
Principal Deputy
Deputy Director for Information Security
Deputy Director for Personnel Security
Deputy Director for Operations Security & RTP
Deputy Director for Program Integration
Deputy Director for Physical Security

Security Vision and Goals

VISION

A secure DoD guided by sound, comprehensive, and adaptable security policy

GOALS

Government leader in security policy, Current and relevant security policy, Effective outreach and oversight program to improve security policy and implementation, Improved competency and professionalization of security career field, A Security Directorate resourced and staffed for mission success, A Security Directorate where we nurture and develop each other for optimum success.

"The Right Policy at the Right Time"

Information Security Responsibilities

- Policy
  - Publish Issuances
  - Represent DoD on Various Policy Forums
  - Staff Waiver Requests
  - Address Policy Issues
- Oversight
  - Visits
  - Data Calls

Key Issuances

- DoD Directive 5200.1 Information Security
- DoD 5200.1-R Information Security Program
  - Declassification Marking Guidance for DoD Special Access Program (SAP) Classified Material, April 26, 2007
  - Under Secretary of Defense for Intelligence Memorandum, "Use of the "Not Releasable to Foreign Nationals" (NOFORN) Caveat on Department of Defense (DoD) Information," May 17, 2005
  - Security Classification Marking Instructions, September 27, 2004
  - Interim Information Security Guidance, April 16, 2004
- DoD 5200.1-I Index of Security Classification Guides

Information Security Role in the ISE

- Same Rules Apply—Problems in Application
- Special Emphasis on:
  - Classification
  - Markings
  - Access
  - Controlled Unclassified Information (CUI)

ISE Organization

- ISE Leads
  - DNI ISE-PM has the National lead
  - OASD(NII)/DoD CIO has the DoD lead
  - OUSD(I) has the Intelligence and Security lead

Initiatives

- NOFORN Working Group
- Classification Management Working Group
- Marking in an Electronic Environment Working Group
- Classification Marking Implementation Working Group
- Sensitive But Unclassified Coordinating Committee

CUI Background

- Direction
  - Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)
  - Presidential Memo, December 2005, Guideline 3
- Information Sharing Challenge

  Problem: Lack of a uniform government-wide framework for CUI severely impedes information sharing

  Goal: Framework for CUI is essential for creation of an Information Sharing Environment (ISE)

Direction

- Section 1016 of IRTPA
  - "The President shall:
    …create an information sharing environment…
    …ensure that the ISE provides and facilitates the means for sharing …information among all appropriate …entities… through the use of policy guidelines and technologies"

- Guideline 3, Presidential Memo, December 16, 2005
  - "To promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of sensitive but unclassified (SBU) information, …procedures and standards for designating, marking, and handling SBU information … must be standardized across the Federal government."

CUI

Controlled Unclassified Information is…

Unclassified information that does not meet the standard for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interest of the United States or originated by entities outside the U.S. Federal government, and under law or policy requires protection from disclosure, special handling safeguards, and prescribed limits on exchange or dissemination

Reasons for Standardizing CUI Processes

- Presently, CUI is shared according to an ungoverned body of policies and practices that confuse both its producers and users.
- Across the Federal government there are at least **107 unique markings and over 130 different labeling or handling processes and procedures** for CUI.
- Inconsistency in CUI policies **increases the likelihood of erroneous handling and dissemination** of information.

Guideline 3 Status

- Report of SBU CC has been forwarded for Presidential action/approval
- DoD has established CUI Task Force to
  - Develop transition plan
  - Address funding requirements

Your Role

- Honor Markings/Dissemination Statements
- Challenge Markings
- Verify Declassification Instructions before Declassifying Information
- If Originator, Responsible for Markings to include Declassification Instructions

QUESTIONS?

Point of Contact

Ms. Deborah Ross

Office of the Under Secretary of Defense (Intelligence)

703-604-1152

Deborah.Ross@osd.mil